数理解析研究所講究録
第 1630 巻 2009 年 106-121

ＦＴＭゲートを用いた量子アルゴリズムの定式化について

東京理科大学 理工学研究科 情報科学専攻　林田 貴宏 (Takahiro Hayashida)
東京理科大学 理工学部 情報科学科　渡邊　昇 (Noboru Watanabe)
Department of Information Sciences, Faculty of Science and Technology,
Tokyo University of Science

1 はじめに

1982 年, E.Fredkin と T.Toffolin は可逆かつビット保存的なゲートを提案した (以下 FT ゲート). 1989 年, G.J.Milburn は FT ゲートの光学的モデルを考案した. これが FTM ゲートである. 1998 年, Ohya, Watanabe により量子チャネル理論を用いた FTM ゲートの定式化が行われた. その後, 量子チャネル理論や量子情報理論を用いて, 量子コンピューターを構成するゲートとして FTM ゲートに関する研究が進められている. アルゴリズムの分野では 1994 年に P.W.Shor が素因数分解を高速に行える量子アルゴリズムを示した. 古典的なコンピューターにおいては素因数分解を効率的に実行できるアルゴリズムが発見されていないため, 素因数分解に指数時間が必要とされる. 一方, Shor の示したアルゴリズムは, 量子コンピューター上において素因数分解を多項式時間で行うことが可能というものであり, 古典的なコンピューターに比べて飛躍的に短い時間で素因数分解が行えるため大きな注目を集めた. この量子アルゴリズムのアイディアを契機として, 各種の量子アルゴリズムが精力的に研究されている.

現在, FTM ゲートに単一光子を入射するモデルにおいては量子アルゴリズムが実行可能であることが分かっているが, 単一光子はその生成や状態の維持が難しい. そこで, 単一光子以外の光と FTM ゲート用いた場合の量子アルゴリズムの実行可能性について調べることを目的とし, 本研究ではその 1 ステップとして, Shor の素因数分解アルゴリズムを取り上げ, このアルゴリズムを実行可能な回路を FTM ゲートを用いて構成し, 量子チャネルによりこれを定式化することを試みた.

2 量子チャネル

Shor の素因数分解アルゴリズムの前に, まず量子チャネルについて説明する.

$\mathcal{H}_1$,$\mathcal{H}_2$ を複素ヒルベルト空間とし, $\mathrm{B}(\mathcal{H}_k)$ を $\mathcal{H}_k$ $(k=1,2)$ 上の有界線形作用素の全体とする. $\mathfrak{S}(\mathcal{H}_k)$ は $\mathcal{H}_k$ 上の密度作用素の全体で, 次のようなものである.

$$\mathfrak{S}(\mathcal{H}_k)=\{\rho\in\mathrm{B}(\mathcal{H}_k)\mid\rho\geq0,\mathrm{tr}\rho=1\}$$

$\mathfrak{S}(\mathcal{H}_1)$ から $\mathfrak{S}(\mathcal{H}_2)$ への写像 Λ^* を量子チャネルという. Λ^* がアフィン性を満たすとき, すなわち

$$\sum_n\lambda_n=1\,(\forall\rho\geq0)$$

であるとき, $\forall\rho_n\in\mathfrak{S}(\mathcal{H}_1)$ について

$$\Lambda^*\left(\sum_n\lambda_n\rho_n\right)=\sum_n\lambda_n)\Lambda^*(\rho_n)$$

となるならば, Λ^* を線形な量子チャネルという. 写像 $\Lambda:\mathrm{B}(\mathcal{H}_2)\to\mathrm{B}(\mathcal{H}_1)$ が $\forall\rho\in\mathfrak{S}(\mathcal{H}_1),\forall A\in\mathrm{B}(\mathcal{H}_2)$ について,

$$\mathrm{tr}\Lambda^*(\rho)A=\mathrm{tr}\rho\Lambda(A)$$

であるとき, Λ を Λ^* の共役写像であるという. さらに Λ が $\forall n\in\mathrm{N},\forall A_j\in\mathrm{B}(\mathcal{H}_2),\forall B_k\in\mathrm{B}(\mathcal{H}_1)$ について

$$\sum_{j,k=1}^n B_j^*\Lambda\left(A_j^*A_k\right)B_k\geq0$$

を満たす場合, Λ は完全正写像であり, Λ^* を完全正チャネルと呼ぶ.

3 Shor の因数分解アルゴリズム

3.1 Shor の因数分解アルゴリズムの量子チャネル表現

文献 [10] に基づき, 量子チャネルにより表わされた Shor の因数分解アルゴリズムを説明する. なお, 基本的なアイディアは Shor の手法に基づくが, 細かい部分では異なる部分があることをお断りしておく.

まず, 因数分解する数を $X\in\mathbb{N}$ とする. $X^2\leq2^N<2X^2$ を満たす整数 N を選び, $Y<X$ かつ $\gcd(Y,X)=1$ となる Y を適当に選ぶ.

次に, $\mathcal{H}=\bigotimes_1^N\mathbb{C}^2$ 上の $\mathrm{CONS}\{|r_k\rangle\}$ を用意して N-qbit のレジスタとする. レジスタの値が $k=2^{N-1}k_{N-1}+2^{N-2}k_{N-2}+\cdots+2k_1+k_0$ であるときレジスタの状態は

$$|r_k\rangle=|k_{N-1}\rangle\otimes|k_{N-2}\rangle\otimes\cdots\otimes|k_0\rangle$$

である．各 $|k_i\rangle$ はレジスタを構成する qbit にあたり，$\mathbb{C}^2$ 上の適当な CONS を $\{|0\rangle, |1\rangle\}$ として qbit の状態を表すものである．

初期状態を $\rho_0 = |r_0\rangle\langle r_0|$ とする．ここで写像 $\Lambda_F^* : \mathfrak{S}(\mathcal{H}) \to \mathfrak{S}(\mathcal{H})$ を次のように定める．

$$\Lambda_F^*(\rho) = \sum_{k,k'} U_f(k) P_k \rho P_{k'} U_f^*(k')$$

$$P_k = |r_k\rangle\langle r_k|$$

$$U_f(t)|r_t\rangle = \frac{1}{\sqrt{2^N}} \sum_{k=0}^{2^N-1} \exp\left(\frac{2\pi itk}{2^N}\right)|r_k\rangle$$

このチャネルは離散フーリエ変換に対応する．さらに写像 $\Lambda_L^* : \mathfrak{S}(\mathcal{H}) \to \mathfrak{S}(\mathcal{H} \otimes \mathcal{K})$ を

$$\Lambda_L^*(\rho) = \sum_{k,k'=0}^{2^N-1} P_k \rho P_{k'} \otimes |s_{m(k)}\rangle\langle s_{m(k)'}| \qquad \left(m(k) = Y^k \mod X\right)$$

とする．ここに $\mathcal{K} = \bigotimes_1^{N'} \mathbb{C}^2$ であり，$\mathcal{K}$ は第 2 レジスタを表す．第 2 レジスタの状態 $|s_i\rangle$ は，第 1 レジスタと同様に考えてよい．また，第 2 レジスタ $(\mathcal{K})$ の観測チャネルを

$$\Lambda_{O\mathcal{K}}^*(\rho) = \sum_{i=0}^{2^{N'}-1} (I \otimes Q_i)\rho(I \otimes Q_i^*) \qquad (Q_i = |s_i\rangle\langle s_i|, \rho \in \mathfrak{S}(\mathcal{H} \otimes \mathcal{K}))$$

第 1 レジスタ $(\mathcal{H})$ の観測チャネルを

$$\Lambda_{O\mathcal{H}}^*(\rho) = \sum_{i=0}^{2^N-1} P_i \rho P_i^* \qquad (\rho \in \mathfrak{S}(\mathcal{H}))$$

とする．このとき Shor の素因数分解アルゴリズムを表す量子チャネルは次のように書ける．

$$\Lambda_S^*(\rho_0) = \Lambda_{O\mathcal{H}}^*(\Lambda_F^*(\mathrm{tr}_{\mathcal{K}}\Lambda_{O\mathcal{K}}^*(\Lambda_L^*(\Lambda_F^*(\rho_0)))))$$

量子チャネルとして表された Shor の素因数分解アルゴリズムでは Λ_F^*, Λ_L^*, $\mathrm{tr}_{\mathcal{K}}$, $\Lambda_{O\mathcal{H}}^*$, $\Lambda_{O\mathcal{K}}^*$ といった写像が用いられている．これらの中で $\Lambda_{O\mathcal{H}}^*$ と $\Lambda_{O\mathcal{K}}^*$ は観測を行う過程であり，この動作は論理ゲートや論理回路とは趣が異なる．ひとまず今の段階では FTM ゲートから出力された光の状態は観測できるものとして深く立ち入らないことにする．さて，Λ_s^* を構成する 5 つの写像の中で論理回路に相当する部分は Λ_F^* と Λ_L^* である．出力状態を適切に観測できるとし，Λ_F^* と Λ_L^* に相当する回路を FTM ゲートを用いて構成することができれば，Λ_s^* を FTM ゲートを基にした論理回路で置き換えることができる．

3.2 Shor の素因数分解アルゴリズムに用いられるゲート

前節では Shor の素因数分解アルゴリズムの全体を見た．この節では Shor の素因数分解アルゴリズムを実行可能な回路を構成するために必要となるゲートについて述べる．

量子計算過程はユニタリー作用素で記述される．任意のユニタリー変換に対応するゲートが得られればどんな量子計算回路でも作ることができるが，物理的な条件を考慮すると作ることのできるゲートは限られてくる．このため限られたゲートの組み合わせで回路を構成する必要がある．

まず，Λ_L^* について考える．Λ_L^* の動作は第 1 レジスタの状態 $|r_k\rangle$ に対して，第 2 レジスタの状態を $|s_i\rangle$ $\left(i = Y^k \mathrm{mod} X\right)$ に対応させるものである．k から $i = Y^k \mathrm{mod} X$ を得る計算過程は少なからず考えられるが，そのうちの 1 つは古典的なコンピューターのように数を 2 進のビット列で表し，レジスタのビット操作を繰り返すことで $j = Y^k \mathrm{mod} X$ を得る方法である．古典的なコンピューターにおける任意のビット操作回路は，量子計算回路において，CNOT ゲートの組み合わせで構成できる．つまり，FTM ゲートが CNOT ゲートとして動作するならば Λ_L^* は FTM ゲートの組み合わせで回路を構成できることになる．

ヒルベルト空間 $\mathbb{C}^2$ 上の CONS を $\{\,|\,0\rangle, |\,1\rangle\,\}$ とする．このとき CNOT ゲートは $\mathbb{C}^2 \otimes \mathbb{C}^2$ 上のユニタリー作用素として次のように書ける．

$$U_{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes (|0\rangle\langle 1| + |1\rangle\langle 0|)$$

なお，CNOT ゲートを表すユニタリーチャネルは次のように書ける．

$$\Lambda_{CNOT}^*(\cdot) = U_{CNOT}(\cdot)U_{CNOT}^*$$

次に Λ_F^* について考える．Λ_F^* の操作は量子離散フーリエ変換である．量子離散フーリエ変換において必要となるゲートはアダマールゲートと制御位相シフトゲートである．制御位相シフトゲートは CNOT ゲートと単一 qbit の位相シフトゲートの組み合わせで構成できる．よって，アダマールゲート，位相シフトゲート，CNOT ゲートを FTM ゲートで構成することができれば，FTM ゲート組み合わせることで量子離散フーリエ変換回路を構成できることになる．

アダマールゲートを表すユニタリー作用素は次のように書ける．

$$U_H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|)$$

位相シフトゲートは $\omega \in \mathbb{R}$ として

$$U_{PS} = |0\rangle\langle 0| + e^{i\omega}|1\rangle\langle 1|$$

となる．

4 光の状態

FTM ゲートに用いる光の状態の定式化について [12] に従って説明する.

4.1 光子数確定状態

a, a^* をそれぞれ光子の消滅作用素, 生成作用素とする. $\hbar\omega = 1$ としたときに, 調和振動子のハミルトニアンは

$$H = \left(a^* a + \frac{I}{2}\right)$$

で与えられる. H の固有ベクトル E_n に対応する固有ベクトルを x_n とすると

$$Hx_n = E_n x_n$$

$$E_n = n + \frac{1}{2} \quad (n = 1, 2, 3, \cdots)$$

である. 各 E_n に対応する固有ベクトル x_n の集合は CONS を成すので, $|n\rangle = x_n$ として CONS$\{|n\rangle : (n = 0, 1, 2, \cdots)\}$ を作ることができ, $|n\rangle$ を n 光子数確定状態ベクトルと呼ぶ. 状態ベクトル $|n\rangle$ を用いて

$$F_n = |n\rangle\langle n|$$

と表される状態を n 光子数確定状態という.

4.2 コヒーレント状態

コヒーレント状態ベクトルは, 消滅作用素 a の固有値 θ に関する固有状態ベクトルとして得ることができ

$$a\,|\theta\rangle = \theta\,|\theta\rangle$$

なる固有ベクトル $|\theta\rangle$ がコヒーレント状態ベクトルである. $|\theta\rangle$ を光子数確定状態を含む CONS$\{|n\rangle\}$ でフーリエ展開すると

$$|\theta\rangle = \exp\{-\frac{1}{2}|\theta|^2\} \sum_{n=0}^{\infty} \frac{\theta^n}{\sqrt{n!}}\,|n\rangle$$

となる. $|\theta\rangle$ を用いて

$$\rho = |\theta\rangle\langle\theta|$$

と表される状態が, コヒーレント状態である [13].

4.3 Schrödinger cat states

コヒーレント状態 $|\theta\rangle\langle\theta|$ と $|-\theta\rangle\langle-\theta|$ により与えられる状態

$$\rho = \frac{1}{2}|\theta\rangle\langle\theta| + \frac{1}{2}|-\theta\rangle\langle-\theta|$$

のシャッテン分解は, 固有値

$$\mu_0 = \frac{1}{2}\left(1+\exp\left(-2|\theta|^2\right)\right)$$
$$\mu_1 = \frac{1}{2}\left(1-\exp\left(-2|\theta|^2\right)\right)$$

と, 固有ベクトル

$$|\phi_+^\theta\rangle = \frac{1}{\tau_+^\theta}\left(|\theta\rangle + |-\theta\rangle\right) \qquad \left(\frac{1}{\tau_+^\theta} = \frac{1}{\sqrt{2\left(1+\exp\left(-2|\theta|^2\right)\right)}}\right)$$

$$|\phi_-^\theta\rangle = \frac{1}{\tau_-^\theta}\left(|\theta\rangle - |-\theta\rangle\right) \qquad \left(\frac{1}{\tau_-^\theta} = \frac{1}{\sqrt{2\left(1-\exp\left(-2|\theta|^2\right)\right)}}\right)$$

によって

$$\rho = \sum_{i=0}^{1}\mu_i\,|s_i\rangle\langle s_i|$$

となる.

$$\langle s_i|s_j\rangle = \delta_{ij}$$

となるため, $|\phi_+\rangle$, $|\phi_-\rangle$ は直交状態ベクトルであり, 特に Schrödinger cat state ベクトルと呼ぶ. 状態

$$\Phi_0 = |\phi_+\rangle\langle\phi_+|$$
$$\Phi_1 = |\phi_-\rangle\langle\phi_-|$$

を Schrödinger cat states という. $|\phi_+\rangle$, $|\phi_-\rangle$ を光子数確定状態を含む CONS$\{|n\rangle\}$ でフーリエ展開すると

$$|\phi_+^\theta\rangle = \frac{\sqrt{2}\exp\left(-\frac{1}{2}|\theta|^2\right)}{\sqrt{1+\exp\left(-2|\theta|^2\right)}}\sum_{n=0}^{\infty}\frac{\theta^{2n}}{\sqrt{2n!}}|2n\rangle$$
$$|\phi_-^\theta\rangle = \frac{\sqrt{2}\exp\left(-\frac{1}{2}|\theta|^2\right)}{\sqrt{1+\exp\left(-2|\theta|^2\right)}}\sum_{n=0}^{\infty}\frac{\theta^{2n+1}}{\sqrt{(2n+1)!}}|2n+1\rangle$$

となる．このことから $|\phi_+\rangle$ は偶数の光子数確定状態ベクトルのみからなる重ね合わせ状態ベクトルで，$|\phi_-\rangle$ は奇数の光子数確定状態ベクトルからなる重ね合わせ状態ベクトルであることがわかる．

5 FTM ゲート

FTM ゲートは入力 1，入力 2，制御の 3 つの入力と，出力 1，出力 2，制御の 3 つの出力を持つ 3 入力 3 出力のゲートである．FTM ゲートの動作は，制御が 0 のとき入力 1 と入力 2 の状態をそのまま出力 1，出力 2 へ出力し，制御が 1 のとき入力 1 を出力 2 へ，入力 2 を出力 1 へと状態を交換して出力するというものである．この動作から FTM ゲートの逆ゲートは FTM ゲートそれ自身である．

5.1 一般化されたビームスプリッター

文献 [5][11][12] に従い，ビームスプリッターについて説明する．入力系を $\mathcal{H}_1$，出力系を $\mathcal{H}_2$，雑音系を $\mathcal{K}_1$，損失系を $\mathcal{K}_2$ とし，$\mathcal{H}_1 \otimes \mathcal{K}_1$ から $\mathcal{H}_2 \otimes \mathcal{K}_2$ への線形変換 V を次のように定める．

$$V\left(|n_1\rangle \otimes |m_1\rangle\right) = \sum_{j=0}^{n_1+m_1} C_j^{n_1 m_1} |n_1 + m_1 - j\rangle \otimes |j\rangle$$

ここに，

$$C_j^{n_1 m_1} \equiv \sum_{r=L}^{K} (-1)^{n_1 - r} \frac{\sqrt{n_1! m_1! j! \,(n_1 + m_1 - j)!}}{r!\,(n_1 - r)!\,(j - r)!\,(m_1 - j + r)!} \alpha^{m_1 - j + 2r} \beta^{n_1 + j - 2r}$$
$$(K = min\{j, n_1\}, L = max\{j - m_1, 0\})$$

である．V を用いて $\mathfrak{S}\left(\mathcal{H}_1 \otimes \mathcal{K}_1\right)$ から $\mathfrak{S}\left(\mathcal{H}_2 \otimes \mathcal{K}_2\right)$ への完全正な量子チャネル Π_{BS}^* が

$$\Pi_{BS}^*\left(\cdot\right) \equiv V\left(\cdot\right) V^*$$

と定められる．この Π_{BS}^* はビームスプリッターを表すチャネルであり，$|\alpha|^2 = \eta$ とおくと，η はビームスプリッターの透過率と見なすことができる．

5.2 光 Kerr 効果

光 Kerr 効果は制御光の強度によって屈折率が変化する相互位相変調である．光 Kerr 効果は複素ヒルベルト空間 $\mathcal{L}_1$，$\mathcal{L}_2$ をそれぞれ制御光の入力系，出力系とし，$\mathcal{H}_1$，$\mathcal{H}_2$ を変調を受ける光の入力系，出力系としたとき，$\mathfrak{S}\left(\mathcal{L}_1 \otimes \mathcal{H}_1\right)$ から $\mathfrak{S}\left(\mathcal{L}_2 \otimes \mathcal{H}_2\right)$ への量子

チャネルとして記述できる. Kerr 効果を表す相互作用ハミルトニアンは次のように与えられる [4][9][13].

$$H_{int} = \hbar\chi\left(N_{c_1} \otimes N_{a_1}\right)$$

N_{c_1}, N_{a_1} はそれぞれ $\mathcal{L}_1$, $\mathcal{H}_1$ の光子数作用素であり, χ は媒質の性質によって定まる定数である. 相互作用を表すユニタリー作用素 U は H_{int} を用いて

$$U_K = \exp\left\{-i\sqrt{F}\left(N_{c_1} \otimes N_{a_1}\right)\right\}$$

と与えられる. ここに $\sqrt{F} = \chi T$ であり, T は光が媒質を通過するのにかかる時間である. $\sqrt{F}$ は光 Kerr 効果による相互作用の強さを表すパラメータとなる. U を用いて光 Kerr 効果を表す量子チャネルは次のように書ける.

$$\Lambda_K^*\left(\cdot\right) \equiv U_K\left(\cdot\right)U_K^*$$

5.3 FTM ゲートのチャネル表現

文献 [11][14] に従い, 5.1 及び 5.2 で定式化したビームスプリッターと光 Kerr 効果の量子チャネルを用いて, FTM ゲートを量子力学的チャネルとして定式化する. FTM ゲートの 3 つの入力について, 制御系を $\mathcal{L}_1$, 入力系 1 を $\mathcal{H}_1$, 入力系 2 を $\mathcal{K}_1$, 同様に出力系を $\mathcal{L}_4$, $\mathcal{H}_4$, $\mathcal{K}_4$ としたとき, FTM ゲートは $\mathfrak{S}\left(\mathcal{L}_1 \otimes \mathcal{H}_1 \otimes \mathcal{K}_1\right)$ から $\mathfrak{S}\left(\mathcal{L}_4 \otimes \mathcal{H}_4 \otimes \mathcal{K}_4\right)$ への写像

$$\Lambda_{FTM}^*\left(\cdot\right) = \Lambda_{BS2}^* \circ \Lambda_K^* \circ \Lambda_{BS1}^*\left(\cdot\right)$$

として記述される.

FTM ゲートに Schrödinger cat state 光を入力した場合,

$$\begin{aligned}
\Lambda_{PS}^*\left(\Phi_- \otimes \Phi_\pm \otimes \Phi_\pm\right) &= \Phi_- \otimes \Phi_\mp \otimes \Phi_\mp \\
\Lambda_{PS}^*\left(\Phi_- \otimes \Phi_\mp \otimes \Phi_\pm\right) &= \Phi_- \otimes \Phi_\pm \otimes \Phi_\mp \\
\Lambda_{PS}^*\left(\Phi_+ \otimes \Phi_\pm \otimes \Phi_\pm\right) &= \Phi_+ \otimes \Phi_\pm \otimes \Phi_\pm \\
\Lambda_{PS}^*\left(\Phi_+ \otimes \Phi_\mp \otimes \Phi_\pm\right) &= \Phi_+ \otimes \Phi_\mp \otimes \Phi_\pm
\end{aligned}$$

(複号同順)

となり, 極めて理想的な動作が期待できる.

6 FTM ゲートの動作

この節では FTM ゲートが CNOT ゲート, アダマールゲート, 位相シフトゲートとして成り立つかを見る. なお以下断らない限り $|\cdot\rangle$ は光の状態ベクトルとし, ビットの状態としての 0,1 はそれぞれ $|0\rangle_{bit}$, $|1\rangle_{bit}$ と表すことにする.

6.1 FTM ゲートによるアダマールゲート

$\alpha = \beta = \frac{1}{\sqrt{2}}$ のハーフビームスプリッターに Schrödinger cat state 光を入射する.

$$
\begin{aligned}
V_{BS}\left(\left|\phi_+^\theta\right\rangle \otimes \left|\phi_-^\theta\right\rangle\right) &= V_{BS}\left(\frac{1}{\tau_+^\theta \tau_-^\theta}\left(|\theta\rangle + |-\theta\rangle\right) \otimes \left(|\theta\rangle - |-\theta\rangle\right)\right) \\
&= \frac{1}{\tau_+^\theta \tau_-^\theta} V_{BS}\left(|\theta\rangle \otimes |\theta\rangle - |\theta\rangle \otimes |-\theta\rangle + |-\theta\rangle \otimes |\theta\rangle - |-\theta\rangle \otimes |-\theta\rangle\right) \\
&= \frac{1}{\tau_+^\theta \tau_-^\theta}\Big(|0\rangle \otimes \left|\sqrt{2}\theta\right\rangle - \left|-\sqrt{2}\theta\right\rangle \otimes |0\rangle \\
&\quad + \left|\sqrt{2}\theta\right\rangle \otimes |0\rangle - |0\rangle \otimes \left|-\sqrt{2}\theta\right\rangle\Big) \\
&= \frac{1}{\tau_+^\theta \tau_-^\theta}\left(|0\rangle \otimes \left(|\sqrt{2}\theta\rangle - |-\sqrt{2}\theta\rangle\right) + \left(|\sqrt{2}\theta\rangle - |-\sqrt{2}\theta\rangle\right) \otimes |0\rangle\right) \\
&= \frac{1}{\sqrt{2}}\Bigg(|0\rangle \otimes \sqrt{\frac{2}{\tau_+^\theta \tau_-^\theta}}\left(|\sqrt{2}\theta\rangle - |-\sqrt{2}\theta\rangle\right) \\
&\quad + \sqrt{\frac{2}{\tau_+^\theta \tau_-^\theta}}\left(|\sqrt{2}\theta\rangle - |-\sqrt{2}\theta\rangle\right) \otimes |0\rangle\Bigg) \\
&= \frac{1}{\sqrt{2}}\left(|0\rangle \otimes \left|\phi_-^{\sqrt{2}\theta}\right\rangle + \left|\phi_-^{\sqrt{2}\theta}\right\rangle \otimes |0\rangle\right)
\end{aligned}
$$

ここで,

$$
\begin{aligned}
|0\rangle &= \frac{1}{\sqrt{2\left(1 + \exp\left(-2|0|^2\right)\right)}}\left(|0\rangle + |-0\rangle\right) \\
&= \left|\phi_+^0\right\rangle
\end{aligned}
$$

であるから,

$$
V_{BS}\left(\left|\phi_+^\theta\right\rangle \otimes \left|\phi_-^\theta\right\rangle\right) = \frac{1}{\sqrt{2}}\left(\left|\phi_+^0\right\rangle \otimes \left|\phi_-^{\sqrt{2}\theta}\right\rangle + \left|\phi_-^{\sqrt{2}\theta}\right\rangle \otimes \left|\phi_+^0\right\rangle\right)
$$

となる. また,

$$
\begin{aligned}
V_{BS}\left(\left|\phi_-^\theta\right\rangle \otimes \left|\phi_+^\theta\right\rangle\right) &= V_{BS}\left(\frac{1}{\tau_+^\theta \tau_-^\theta}\left(|\theta\rangle - |-\theta\rangle\right) \otimes \left(|\theta\rangle + |-\theta\rangle\right)\right) \\
&= \frac{1}{\tau_+^\theta \tau_-^\theta} V_{BS}\left(|\theta\rangle \otimes |\theta\rangle + |\theta\rangle \otimes |-\theta\rangle - |-\theta\rangle \otimes |\theta\rangle - |-\theta\rangle \otimes |-\theta\rangle\right) \\
&= \frac{1}{\tau_+^\theta \tau_-^\theta}\Big(|0\rangle \otimes \left|\sqrt{2}\theta\right\rangle + \left|-\sqrt{2}\theta\right\rangle \otimes |0\rangle \\
&\quad - \left|\sqrt{2}\theta\right\rangle \otimes |0\rangle - |0\rangle \otimes \left|-\sqrt{2}\theta\right\rangle\Big)
\end{aligned}
$$

$$= \frac{1}{\tau_+^\theta \tau_-^\theta}\left(|0\rangle \otimes \left(|\sqrt{2}\theta\rangle - |-\sqrt{2}\theta\rangle\right) - \left(|\sqrt{2}\theta\rangle - |-\sqrt{2}\theta\rangle\right) \otimes |0\rangle\right)$$
$$= \frac{1}{\sqrt{2}}\left(|0\rangle \otimes \sqrt{\frac{2}{\tau_+^\theta \tau_-^\theta}}\left(|\sqrt{2}\theta\rangle - |-\sqrt{2}\theta\rangle\right) \right.$$
$$\left. - \sqrt{\frac{2}{\tau_+^\theta \tau_-^\theta}}\left(|\sqrt{2}\theta\rangle - |-\sqrt{2}\theta\rangle\right) \otimes |0\rangle\right)$$
$$= \frac{1}{\sqrt{2}}\left(|\phi_+^0\rangle \otimes \left|\phi_-^{\sqrt{2}\theta}\right\rangle - \left|\phi_-^{\sqrt{2}\theta}\right\rangle \otimes |\phi_+^0\rangle\right)$$

さらに，$|\phi_+^0\rangle \otimes \left|\phi_-^{\sqrt{2}\theta}\right\rangle$ と $\left|\phi_-^{\sqrt{2}\theta}\right\rangle \otimes |\phi_+^0\rangle$ をハーフビームスプリッターに通した場合の出力を調べる．

$$\begin{aligned}
V_{BS}\left(|\phi_+^0\rangle \otimes \left|\phi_-^{\sqrt{2}\theta}\right\rangle\right) &= \frac{2}{\tau_+^0 \tau_-^{\sqrt{2}\theta}} V_{BS}\left(|0\rangle \otimes \left(|\sqrt{2}\theta\rangle - |-\sqrt{2}\theta\rangle\right)\right) \\
&= \frac{2}{\tau_+^0 \tau_-^{\sqrt{2}\theta}} V_{BS}\left(\left(|0\rangle \otimes |\sqrt{2}\theta\rangle - |0\rangle \otimes |-\sqrt{2}\theta\rangle\right)\right) \\
&= \frac{2}{\tau_+^0 \tau_-^{\sqrt{2}\theta}} \left(|\theta\rangle \otimes |\theta\rangle - |-\theta\rangle \otimes |-\theta\rangle\right) \\
&= \frac{1}{\tau_+^0 \tau_-^{\sqrt{2}\theta}} \left(\left(|\theta\rangle + |-\theta\rangle\right) \otimes \left(|\theta\rangle - |-\theta\rangle\right)\right. \\
&\quad \left. + \left(\left(|\theta\rangle - |-\theta\rangle\right) \otimes \left(|\theta\rangle + |-\theta\rangle\right)\right)\right) \\
&= \frac{1}{\tau_+^0 \tau_-^{\sqrt{2}\theta}} \tau_+^\theta \tau_-^\theta \left(|\phi_+^\theta\rangle \otimes |\phi_-^\theta\rangle + |\phi_-^\theta\rangle \otimes |\phi_+^\theta\rangle\right) \\
&= \frac{1}{\sqrt{2}} \left(|\phi_+^\theta\rangle \otimes |\phi_-^\theta\rangle + |\phi_-^\theta\rangle \otimes |\phi_+^\theta\rangle\right)
\end{aligned}$$

$$\begin{aligned}
V_{BS}\left(\left|\phi_-^{\sqrt{2}\theta}\right\rangle \otimes |\phi_+^0\rangle\right) &= \frac{2}{\tau_+^0 \tau_-^{\sqrt{2}\theta}} V_{BS}\left(\left(|\sqrt{2}\theta\rangle - |-\sqrt{2}\theta\rangle\right) \otimes |0\rangle\right) \\
&= \frac{2}{\tau_+^0 \tau_-^{\sqrt{2}\theta}} V_{BS}\left(\left(|\sqrt{2}\theta\rangle \otimes |0\rangle - |-\sqrt{2}\theta\rangle \otimes |0\rangle\right)\right) \\
&= \frac{2}{\tau_+^0 \tau_-^{\sqrt{2}\theta}} \left(|-\theta\rangle \otimes |\theta\rangle - |\theta\rangle \otimes |-\theta\rangle\right) \\
&= \frac{1}{\tau_+^0 \tau_-^{\sqrt{2}\theta}} \left(\left(|\theta\rangle + |-\theta\rangle\right) \otimes \left(|\theta\rangle - |-\theta\rangle\right)\right. \\
&\quad \left. - \left(\left(|\theta\rangle - |-\theta\rangle\right) \otimes \left(|\theta\rangle + |-\theta\rangle\right)\right)\right) \\
&= \frac{1}{\tau_+^0 \tau_-^{\sqrt{2}\theta}} \tau_+^\theta \tau_-^\theta \left(|\phi_+^\theta\rangle \otimes |\phi_-^\theta\rangle - |\phi_-^\theta\rangle \otimes |\phi_+^\theta\rangle\right) \\
&= \frac{1}{\sqrt{2}} \left(|\phi_+^\theta\rangle \otimes |\phi_-^\theta\rangle - |\phi_-^\theta\rangle \otimes |\phi_+^\theta\rangle\right)
\end{aligned}$$

ハーフビームスプリッターを 2 回通した出力状態を見る.

$$
\begin{aligned}
&V_{BS} \circ V_{BS} \left(\left| \phi_-^\theta \right\rangle \otimes \left| \phi_+^\gamma \right\rangle \right) \\
&= \frac{1}{\tau_+^\gamma \tau_-^\theta} V_{BS} \circ V_{BS} \left(|\theta\rangle \otimes |\gamma\rangle + |\theta\rangle \otimes |-\gamma\rangle - |-\theta\rangle \otimes |\gamma\rangle - |-\theta\rangle \otimes |-\gamma\rangle \right) \\
&= \frac{1}{\tau_+^\gamma \tau_-^\theta} V_{BS} \left(\left| \frac{1}{\sqrt{2}} (-\theta + \gamma) \right\rangle \otimes \left| \frac{1}{\sqrt{2}} (\theta + \gamma) \right\rangle + \left| \frac{1}{\sqrt{2}} (-\theta - \gamma) \right\rangle \otimes \left| \frac{1}{\sqrt{2}} (\theta - \gamma) \right\rangle \right. \\
&\quad \left. - \left| \frac{1}{\sqrt{2}} (\theta + \gamma) \right\rangle \otimes \left| \frac{1}{\sqrt{2}} (-\theta + \gamma) \right\rangle - \left| \frac{1}{\sqrt{2}} (\theta - \gamma) \right\rangle \otimes \left| \frac{1}{\sqrt{2}} (-\theta - \gamma) \right\rangle \right) \\
&= \frac{1}{\tau_+^\gamma \tau_-^\theta} \left(|\theta\rangle \otimes |\gamma\rangle + |\theta\rangle \otimes |-\gamma\rangle - |-\theta\rangle \otimes |\gamma\rangle - |-\theta\rangle \otimes |-\gamma\rangle \right) \\
&= \left| \phi_-^\theta \right\rangle \otimes \left| \phi_+^\gamma \right\rangle
\end{aligned}
$$

$$
\begin{aligned}
&V_{BS} \circ V_{BS} \left(\left| \phi_+^\theta \right\rangle \otimes \left| \phi_-^\gamma \right\rangle \right) \\
&= \frac{1}{\tau_+^\gamma \tau_-^\theta} V_{BS} \circ V_{BS} \left(|\theta\rangle \otimes |\gamma\rangle - |\theta\rangle \otimes |-\gamma\rangle + |-\theta\rangle \otimes |\gamma\rangle - |-\theta\rangle \otimes |-\gamma\rangle \right) \\
&= \frac{1}{\tau_+^\gamma \tau_-^\theta} V_{BS} \left(\left| \frac{1}{\sqrt{2}} (-\theta + \gamma) \right\rangle \otimes \left| \frac{1}{\sqrt{2}} (\theta + \gamma) \right\rangle - \left| \frac{1}{\sqrt{2}} (-\theta - \gamma) \right\rangle \otimes \left| \frac{1}{\sqrt{2}} (\theta - \gamma) \right\rangle \right. \\
&\quad \left. + \left| \frac{1}{\sqrt{2}} (\theta + \gamma) \right\rangle \otimes \left| \frac{1}{\sqrt{2}} (-\theta + \gamma) \right\rangle - \left| \frac{1}{\sqrt{2}} (\theta - \gamma) \right\rangle \otimes \left| \frac{1}{\sqrt{2}} (-\theta - \gamma) \right\rangle \right) \\
&= \frac{1}{\tau_+^\gamma \tau_-^\theta} \left(|\theta\rangle \otimes |\gamma\rangle - |\theta\rangle \otimes |-\gamma\rangle + |-\theta\rangle \otimes |\gamma\rangle - |-\theta\rangle \otimes |-\gamma\rangle \right) \\
&= \left| \phi_+^\theta \right\rangle \otimes \left| \phi_-^\gamma \right\rangle
\end{aligned}
$$

$\left| \phi_+^\theta \right\rangle \otimes \left| \phi_-^\gamma \right\rangle$ と $\left| \phi_-^{\theta'} \right\rangle \otimes \left| \phi_+^{\gamma'} \right\rangle$ をそれぞれ $|0\rangle_{bit}$, $|1\rangle_{bit}$ と見なすとアダマールゲートとしての動作ができることがわかる. ただし, 1 回ビームスプリッターを通した光の状態を見ると, 入射光と同様に Schrödinger cat state の形は保っているものの, θ, θ', γ, γ' の値が変化してしまうため, 厳密には入力状態とは異なる Schrödinger cat state に変化してしまっている. このためアダマールゲートの動作を正確に再現しているわけではない.

以上より, Schrödinger cat state 光を入射したときハーフビームスプリッターがアダマールゲート相当のゲートとして機能することがわかった. よってアダマールゲートに相当する量子チャネルは次のように書ける.

$$
\Lambda_h^* (\cdot) = V_{hBS} (\cdot) V_{hBS}^*
$$

さて, FTM ゲートにおいて 1 枚目のビームスプリッターをハーフビームスプリッターとし, 2 枚目のビームスプリッターを透過率 0 のフルミラーに置き換える. 制御光が真空状態 $|0\rangle$ かもしくは $|\phi_+\rangle$ であればこの FTM ゲートはコントロールビットを除く他の 2

つの入力についてハーフビームスプリッターに等しい動作をする．すなわち FTM ゲートをベースとしたアダマールゲートの量子チャネルは次のように書ける．

$$\Lambda_H^*(\cdot) = V_{mirror} \circ U_K \circ V_{hBS}(\cdot) V_{hBS}^* \circ U_K^* \circ V_{mirror}^*$$

アダマールゲートには $|\phi_+\rangle \otimes |\phi_-\rangle$ と $|\phi_-\rangle \otimes |\phi_+\rangle$ これらの状態を入出力が必要となるので, qbit は 2 つの光のテンソル積として表すことにする．

6.2 FTM ゲートによる CNOT ゲート

CNOT ゲートはコントロールビットが $|0\rangle_{bit}$ であるときは素通りさせ, コントロールビットが $|1\rangle_{bit}$ であるときターゲットビットの $|0\rangle_{bit}$ と $|1\rangle_{bit}$ を反転させる動作をする．このようなゲートは FTM ゲートの振る舞いから直ちに可能であることがわかる．$|\phi_+\rangle \otimes |\phi_-\rangle$ と $|\phi_-\rangle \otimes |\phi_+\rangle$ をそれぞれ $|0\rangle_{bit}$, $|1\rangle_{bit}$ と見なして入力 1,2 に入射し, コントロールビットにはテンソル積の左側の光, $|0\rangle_{bit}$ であれば $|\phi_+\rangle$, $|1\rangle_{bit}$ であれば $|\phi_-\rangle$ を入射することで CNOT ゲートとして動作する．

このゲートでは入力光が 4 系統になるため, FTM ゲートの量子チャネルに恒等チャネル I を加えて, そこにコントロールビットのテンソル積右側のペアを通すことにする．

$$\Lambda_{CN}^*(\cdot) = I \otimes \Lambda_{FTM}^*(\cdot)$$

6.3 FTM ゲートによる位相シフトゲート

現段階においては Schrödinger cat state 光と FTM ゲートを用いて効果的に位相を変化させる方法は見つかっていない．この原因は Kerr 媒質における被制御光がコヒーレント光であるとき,

$$U_K(|n\rangle \otimes |\theta\rangle) = |n\rangle \otimes \left|e^{-i\sqrt{F}n}\theta\right\rangle$$

このように, 状態 $|\theta\rangle$ に対する位相ではなく, コヒーレント状態光のパラメーターとしての θ を操作してしまうためである．コヒーレント光をベースに作られる Schrödinger cat state 光も同様の問題を抱えている．

ここでは光子の消滅作用素 a を用いて天下り的に位相シフトゲートを構成してしまうことにする．

$$U_{ps}(\cdot) = e^{ia}(\cdot)$$

この作用素を用いると

$$\begin{aligned} U_{ps}(|\theta\rangle) &= e^{ia}|\theta\rangle \\ &= e^{i\theta}|\theta\rangle \end{aligned}$$

となり，θ を適当に操作することで位相シフト操作を得る．なお，$|\theta\rangle$ の代わりに $\left|\phi_{+}^{\theta}\right\rangle$ でも同様に $e^{i\theta}$ を得られる．量子チャネルは次のようになる．

$$\Lambda_{ps}^{*}(\cdot)=U_{ps}(\cdot)\,U_{ps}^{*}$$

ところが，このままでは入力される全ての光に位相シフトを施してしまう．位相シフトゲートは $|0\rangle_{bit}$ について素通りさせ，$|1\rangle_{bit}$ に対してのみ位相を操作できなければならない．このため，定常な入力光 $|0\rangle\otimes|\theta\rangle$ を用い，FTM ゲートを 2 つ組み合わせ，$|1\rangle_{bit}$ に対応する光にのみ位相シフトを施すようにする．

よって位相シフトゲートの量子チャネルは次のようになる．

$$\Lambda_{PS}^{*}(\cdot)=\Lambda_{FTM}^{*}\circ\left(I\otimes\Lambda_{ps}^{*}\otimes I\right)\circ\Lambda_{FTM}^{*}(\cdot)$$

6.4 観測過程

観測過程では，各 qbit について $|0\rangle_{bit}$ か $|1\rangle_{bit}$ が判別できればよい．ここでは $|\phi_{+}\rangle\otimes|\phi_{-}\rangle$ と $|\phi_{-}\rangle\otimes|\phi_{+}\rangle$ を利用して qbit の状態を表現している．単純には 2 系統の光を観測して光子数の偶数，奇数を得ればよいが，$|\phi_{\pm}\rangle$ を観測して得られる可能性のある光子数は多岐に及ぶ上に，光子 1 つ分まで厳密に測定しなければならず，これは現実的でない．このため観測に際して FTM ゲートを用い，2 系統の光のうちどちらか一方を FTM ゲートの制御光として入射させ，他の 2 つの入力には $|0\rangle\otimes|\theta\rangle$ を入射させる．すると qbit の状態に応じて FTM ゲートの出力は $|0\rangle\otimes|\theta\rangle$ もしくは $|\theta\rangle\otimes|0\rangle$ となる．これを観測して各々の qbit の状態を確定させる．

7 FTM ゲートをもとにした Shor の素因数分解回路

これまでに述べた FTM ゲートをもとにしたアダマールゲート，CNOT ゲート，位相シフトゲートを組み合わせて Shor の素因数分解を実行可能な回路を構成する．

7.1 量子離散フーリエ変換回路

N-qbit の量子離散フーリエ変換回路は n 個のアダマールゲートと $\frac{n(n-1)}{2}$ 個の制御位相シフトで構成される．これを量子チャネルで表すと

$$\begin{aligned}\Lambda_{F}^{*}(\cdot)=\ &\Lambda_{H(N)}^{*}\circ\Lambda_{PS(N-1,1)}\circ\Lambda_{H(N-1)}\circ\Lambda_{PS(N-2,2)}\circ\Lambda_{PS(N-2,1)}\circ\Lambda_{H(N-2)}\circ\\&\cdots\circ\Lambda_{PS(2,2)}\circ\Lambda_{PS(2,1)}\circ\Lambda_{H(2)}\circ\Lambda_{PS(1,N)}\circ\Lambda_{PS(1,N-1)}\circ\\&\cdots\circ\Lambda_{PS(1,2)}\circ\Lambda_{PS(1,1)}\circ\Lambda_{H(1)}(\cdot)\end{aligned}$$

となる．

7.2 Modular Exponential 回路

これは Λ_L^* に相当する回路である．まず，2 つの CNOT 回路を用いて 2-qbit の加算回路を作る．

$$\Lambda_{2sum}^*(\cdot) = \Lambda_{FTM}^* \circ \Lambda_{FTM}^*(\cdot)$$

次に 2 つの CCNOT ゲートと 1 つの CNOT を用いて 2-qbit のキャリー回路を作る．CCNOT ゲートは CNOT ゲート 4 つで作ることができる．

$$\Lambda_{2cr}^*(\cdot) = \Lambda_{FTM(9)}^* \circ \Lambda_{FTM(8)}^* \circ \Lambda_{FTM(7)}^* \circ \cdots \circ \Lambda_{FTM(1)}^*(\cdot)$$

2-qbit 加算回路と 2-qbit キャリー回路をもとに N-qbit の加算回路を作る．このためには 2-qbit キャリー回路が n 個，2-qbit キャリー回路の逆回路が n-1 個，2-qbit 加算回路が n 個，CNOT ゲートが必要になる．なお FTM ゲートをもとにした回路の逆回路は逆の順番で FTM ゲートを適用したものである．なお今回定めた位相シフトゲートには FTM ゲートでない部分があるので，その部分については逆回路用のゲートを用意する必要がある．

$$\begin{aligned}\Lambda_{ADD}^*(\cdot) = {} & \Lambda_{2cr(1)}^* \circ \Lambda_{2cr(2)}^* \circ \cdots \circ \Lambda_{2cr(N)}^* \circ \Lambda_{FTM}^* \circ \bar{\Lambda}_{2cr(N)}^* \circ \Lambda_{2sum(N)}^* \circ \\ & \bar{\Lambda}_{2cr(N-1)}^* \circ \Lambda_{2sum(N-1)}^* \circ \cdots \circ \bar{\Lambda}_{2cr(1)}^* \circ \Lambda_{2sum(1)}^*(\cdot)\end{aligned}$$

ここで，FTM ゲートの入力状態の交換を利用した 2 つのレジスタの入れ替えを行う交換ゲートと，読み換えによる COPY 動作を利用してレジスタの値を複製する COPY 回路を用意する．N-qbit の交換ゲートは 2n 個の FTM ゲートで構成でき，それを Λ_{EX}^*，N-qbit の COPY ゲートも 2n 個の FTM ゲートで構成でき，それを Λ_{CP}^* とする．これらを用いて Modular Adder 回路を作る．

$$\begin{aligned}\Lambda_{MA}^*(\cdot) = {} & \Lambda_{ADD(3)}^* \circ \bar{\Lambda}_{ADD(2)}^* \circ \Lambda_{CN}^* \circ \Lambda_{CN}^* \circ \Lambda_{CN}^* \circ \Lambda_{EX(2)}^* \circ \Lambda_{ADD(2)}^* \\ & \Lambda_{EX(1)}^* \circ \bar{\Lambda}_{ADD(1)}^* \circ \Lambda_{CN}^* \circ \Lambda_{ADD(1)}^*(\cdot)\end{aligned}$$

Modular Adder 回路を用いて N-qbit の制御 Modular Multiplexer 回路を作る．

$$\begin{aligned}\Lambda_{CMM}^*(\cdot) = {} & \bar{\Lambda}_{CP(1)}^* \circ \bar{\Lambda}_{MA(1)}^* \circ \cdots \circ \bar{\Lambda}_{CP(N)}^* \circ \bar{\Lambda}_{MA(N)}^* \circ \Lambda_{CN}^* \circ \Lambda_{CN}^* \circ \\ & \bar{\Lambda}_{EX(Nb)}^* \circ \Lambda_{CN}^* \circ \Lambda_{CN}^* \circ \Lambda_{MA(Nb)}^* \circ \Lambda_{CN}^* \circ \Lambda_{CN}^* \circ \bar{\Lambda}_{EX(Na)}^* \circ \\ & \Lambda_{CN}^* \circ \Lambda_{CN}^* \circ \Lambda_{MA(Na)}^* \circ \Lambda_{CP(N)}^* \circ \cdots \circ \Lambda_{CN}^* \circ \Lambda_{CN}^* \circ \bar{\Lambda}_{EX(1b)}^* \circ \\ & \Lambda_{CN}^* \circ \Lambda_{CN}^* \circ \Lambda_{MA(1)}^* \circ \Lambda_{CN}^* \circ \Lambda_{CN}^* \circ \bar{\Lambda}_{EX(1a)}^* \circ \Lambda_{CN}^* \circ \\ & \Lambda_{CN}^* \circ \Lambda_{MA(1)}^* \circ \Lambda_{CP(1)}^*(\cdot)\end{aligned}$$

制御 Modular Multiplexer 回路を使って Modular Exponential 回路, すなわち Λ_L^* を作る.

$$\begin{aligned}\Lambda_L^*(\cdot) &= \Lambda_{ME}^*(\cdot)\\ &= \bar{\Lambda}_{CMM(Nb)}^* \circ \Lambda_{CMM(Nb)}^* \circ \bar{\Lambda}_{CMM(Nb)}^* \circ \Lambda_{EX(Nb)}^* \circ \Lambda_{CMM(Na)}^* \circ \\ &\quad \Lambda_{EX(Na)}^* \circ \cdots \circ \bar{\Lambda}_{CMM(1b)}^* \circ \Lambda_{CMM(1b)}^* \circ \bar{\Lambda}_{CMM(1b)}^* \circ \\ &\quad \Lambda_{EX(1b)}^* \circ \Lambda_{CMM(1a)}^* \circ \Lambda_{EX(1a)}^*(\cdot)\end{aligned}$$

7.3 観測回路

N-qbit のレジスタの観測には N 個の FTM ゲートが必要になる.

$$\Lambda_Q^*(\cdot) = \Lambda_{FTM(N)}^* \circ \Lambda_{FTM(N-1)}^* \circ \Lambda_{FTM(N-2)}^* \circ \cdots \circ \Lambda_{FTM(1)}^*(\cdot)$$

7.4 回路全体

以上より Shor の素因数分解を実行可能な回路は次のように定まる.

$$\Lambda_S^*(\cdot) = \Lambda_{Q(2)}^* \circ \Lambda_{F(2)}^* \circ \Lambda_{Q(1)}^* \circ \Lambda_{ME}^* \circ \Lambda_{F(1)}^*(\cdot)$$

8 まとめ

アダマールゲート, CNOT ゲート, 位相シフトゲートを構成したので, これらを組み合わせれば目的の Shor の素因数分解アルゴリズムを実行する回路の量子チャネルを定めることはできる. しかし, FTM ゲートと Schrödinger cat state 光を用いたモデルにおいて, CNOT ゲートとアダマールゲートに相当するゲートは構成することが可能であることはわかったが, 現在のところ位相シフトを効果的に実行できるゲートの構成法は発見できていない.

今後の課題は, やはり位相シフトゲートの構成である. 位相シフトゲートが実現できなければ回路を構成できない量子アルゴリズムが多いためである. Schrödinger cat state 光を重ね合わせた状態や, Schrödinger cat state 以外の光なども視野にいれて研究を進めていきたい. また, 位相シフトゲートを用いなくても構成可能な回路であれば, FTM ゲートのみから作ることができるため, このような回路についてどの程度の動きが期待できるのかも調べて行きたい.

参考文献

[1] P.W.Shor, Algorithm for quantum computation : Discrete logarithms and factoring algorithm, Proceedings of the 35th Annual IEEE Symposium on Foundation of Computer Science, pp124-134, 1994

[2] R. P. Feynman, "Quantum Mechanical Computers", Optics News, Vol.11,pp.11-20.

[3] E. Fredkin, T. Toffoli, "Conservative Logic", International Journal of Theoretical Physics, Vol.21,pp.219-253, 1982.

[4] G. J. Milburn, "Quantum Optical Fredkin Gate", Phys. Rev. Lett., Vol.62, pp.2124-2127, 1989.

[5] M. Ohya, "On compound state and mutual information in quantum information theory", IEEE Information Theory, 29, 770-774, 1983.

[6] M. Ohya, "Quantum ergodic channels in operator algebras", J.Math.Anal.Appl., 84, No.2.318-327, 1981.

[7] M. Ohya and D. Petz, "Quantum Entropy and its Use", Springer-Verlag, 1993.

[8] M. Ohya, D. Petz and N. Watanabe, "On capacities of quantum channels", Probability and Mathematical Statistics, Vol.17, pp.179-196,1997.

[9] M. Ohya and N. Watanabe, "On Mathmatical Treatment of Fredkin-Toffoli-Milburn Gate", Physica D, 120, pp.206-213, 1998.

[10] 大矢雅則, "量子コンピュータの数理", 丸善, 1999.

[11] 大矢雅則, 渡邉 昇, "量子論的通信過程における数理モデルの形成とその解析", 電子通信学会論文誌, J67-A, No.6, 548-552, 1984.

[12] 大矢雅則, 渡邉 昇, "量子通信論の基礎", 牧野書店, 1998.

[13] D. F. Walls, G. J. Milburn, "Quantum Optics", Springer-Verlag, 1994.

[14] 渡邉 昇, "チャネル理論とその量子コンピュータへの応用", 数理科学 No.402, サイエンス社, 1996.